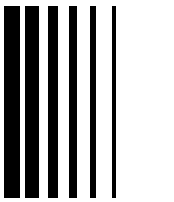

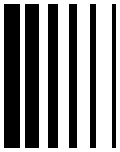

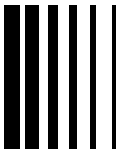

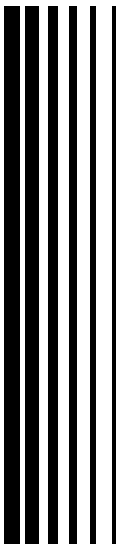

Defense Information Infrastructure (DII) Common Operating Environment (COE) Security Features User's Guide (SFUG) (Final)

22 December 1999

Prepared for:

Joint Interoperability and Engineering Organization
Defense Information Systems Agency

This page intentionally left blank.

Table of Contents

1. INTRODUCTION 1

2. SYSTEM DESCRIPTION 1

2.1 DII COE COMPONENTS 1
2.2 SYSTEM COMPONENTS 2

3. SECURITY PHILOSOPHY 2

3.1 USER RESPONSIBILITIES 2
3.2.1 Least Privilege 3
3.2.2 Security Audit 3
3.2.3 System Integrity Tools 3

4. USER SECURITY GUIDANCE 4

4.1 USER SECURITY FEATURES 4
4.2 IDENTIFICATION AND AUTHENTICATION 4
4.2.1 Password Construction 5
4.2.2 Password Lifetime 6
4.2.3 Password Monitoring 6
4.2.4 Account Lockout 6
4.3 DISCRETIONARY ACCESS CONTROL 6
4.4 USER AUDIT MONITORING 7

5. USER SECURITY ACTIVITIES 7

5.1 UNIX PLATFORMS 7
5.1.1 Logging In to a COE System 7
5.1.2 Logging Off a COE System 8
5.1.3 Changing Passwords 8
5.1.4 Profile Selection 11
5.1.5 File and Directory Permissions 12
5.2 NT PLATFORM 14
5.2.1 Logging In to a COE System 14
5.2.2 Logging Off a COE System 14
5.2.3 Changing Passwords 15
5.2.4 Profile Selection 16
5.2.5 File and Directory Permissions 17
5.3 COE ADMINISTRATIVE DOMAIN 20

PREFACE

The following conventions are used in this document:

Bold	Used for information that is typed, pressed, or selected in executables and instructions. For example, select **connect to host**.
Italics	Used for file names, directories, scripts, commands, user IDs, document names, and Bibliography references; and any unusual computerese. For example, *iconified*, *setup.exe*, *DII/IC Document Delivery and Process and Style Guide*.
Underline	Used for emphasis. Also used for e-mail and web addresses. For example, The user must use these conventions or www.saic.com.
Arrows < >	Used to identify keys on the keyboard. For example, <Return>.
"Quotation Marks"	Used to identify informal, computer-generated queries and reports, or coined names; and to clarify a term when it appears for the first time. For example, "Data-Generation Report".
`Courier Font`	Used to denote commands, command lines, and/or screen dumps as they appear on the screen. For example, `tar xvf dev/rmt/3mm`.
CAPITALIZATION	Used to identify keys, screen icons, screen buttons, field, and menu names. For example, the MAIN MENU button or hit the <F1> key.

1. INTRODUCTION

This *Security Features User's Guide* (SFUG) describes the COE security features available to the user and user security activities and responsibilities within a COE system. This document provides a regular system user with the fundamental information required to access and operate securely in the COE system environment. This document also includes information and recommendations on how to recognize and minimize security risks. Finally, this document augments the security-relevant portions of the commercial off-the-shelf (COTS) manuals for the systems and utilities that comprise the DII COE. Where additional or more detailed information is available, reference is made to the appropriate manual.

2. SYSTEM DESCRIPTION

2.1 DII COE Components

The Defense Information Infrastructure (DII) Common Operating Environment (COE) concept should be thought of as a foundation upon which systems are built. The COE allows for system components to be easily added to the open system in small manageable units defined as segments. The COE concept covers many objectives. A major objective of the COE is to provide a common secure infrastructure for managing software components. This document identifies the user tools for utilizing the security features in the COE 4.x kernel.

The COE is made up of the following components:

- Kernel – the minimal set of software required on a COE workstation. The kernel includes:
  - Operating System & Extensions
  - Common Desktop Environment
  - Software Installation Tools (COE Installer)
  - System and Security Administration Tools
- Infrastructure Services – these include:
  - RDMS Server/clients
  - Networks Management
  - Communications
  - PC Services.
- Common Support Applications – these include:
  - Messaging
  - Office Automation
  - Correlation/fusion
  - Alerts.

2.2 System Components

NOTE: This section should be used by system integrators and/or site administrators to provide additional information for a specific COE system.

3. SECURITY PHILOSOPHY

3.1 User Responsibilities

The fundamental security responsibilities for all COE system users are to:

- Understand the system security features that relate to user activities;
- Maintain the system security configuration for the user's account(s); and
- Report acts of suspected misuse of the system to security staff.

The COE security philosophy is based on a preventative approach that emphasizes system security configuration and control. Properly implemented and monitored, this becomes the first defense against intrusion into and misuse of the system. The COE security configuration is implemented and maintained using a combination of automated security features and procedural (manual) instructions that are enforced by the site security staff.

3.2 COE Security Concepts

The security philosophy underlying the DII COE emphasizes, to the maximum extent possible, reliance upon COTS functionality, within the kernel and Infrastructure Services layer of the COE, for the implementation of security features. For example, this means that access to files and directories is enforced by the underlying operating system and not by GOTS software within the COE. Applications must still be designed appropriately to cooperate with the underlying operating system, but decisions about whether or not a specific user can access a capability is controlled by groups, Access Control Lists (ACLs), etc. as provided by the native operating system. This approach is intentional because it is more cost effective than building Department of Defense (DoD)-unique solutions, because it conforms to accepted commercial standards, and because it prevents the COE from extending the boundaries of the Trusted Computing Base (TCB).

There are a few exceptions to this philosophy in areas where the DII COE Security Engineering Office has determined that commercial solutions are not totally adequate to address DoD concerns. These exceptions, in the present DII COE implementation, are primarily[1] in the areas

[1] Profiling as defined and provided by the COE is *not* intended to be a security enforcement technique. Its purpose is solely to reduce the GUI desktop declutter by displaying only those icons, menus, etc. to the user that the user *should* have access to. Actual granting or denying access to system resources is arbitrated by the underlying operating system, database management system, network software, etc. and not by COE profiling software.

of user account lockout, encryption services for communications, and user inactivity timeouts. Acceptable commercial solutions for these areas are being sought and will eventually replace the present GOTS solutions. Refer to the DII COE Chief Engineer and the *DII COE Buildlist Worksheet* for current status information.

The DII COE security philosophy is based on an approach that emphasizes security configuration and control, then, detection of aberrant activities. System/security administrators will be able to make use of the security features provided by the operating systems, and COTS/GOTS tool products, to aid in the implementation and maintenance of the security configuration.

The security philosophy consists of three principal elements: least privilege, security audit and system integrity tools. The least privilege element is designed to protect the security posture; the security audit and system integrity tools elements are intended to detect and recover from any compromise of the security posture. Each of these elements is explained in the subsections below.

Procedural issues such as proper labeling of electronic media, requirements for maintaining paper trails showing originating authority, etc. are not addressed. These procedural issues lie outside the scope of the DII COE and are more properly addressed by traditional system security policy and Concept of Operations (CONOPS) documents.

3.2.1 Least Privilege

The least privilege concept states that users should be provided with the minimum amount of information or access necessary to perform their specific job functions. For example, files and directories with world-read, -write and –execute permissions do not enforce the least privilege concept. Providing these permissions to the owner of the files and directories, and discrete group access if required (e.g., read permission), would be an example of exercising least privilege. Implementation of the least privilege concept begins with the DII COE kernel, and must be extended to each file that comprises the DII COE (or a specific system such as GCCS) to maintain the security posture. The *DII COE 4.0 I&RTS* mandates the implementation of the least privilege concept through numerous compliance requirements (e.g., the UNIX umask setting of 027).

3.2.2 Security Audit

Users should understand that their activity is audited and that user activity is monitored by the security staff to identify potential system misuse.

3.2.3 System Integrity Tools

The security staff uses a suite of automated security tools to maintain and monitor the security of a COE-based system, and to assist in the recovery of the system in the event of a security violation or compromise. The use of these tools is transparent to the user, but focus on common user activities such as password selection and setting file permissions.

4. USER SECURITY GUIDANCE

This section covers security features of the COE kernel that relate to individual users as well as steps users must take to protect their information.

4.1 User Security Features

The COE security features with which regular users interact or transparently invoke are:

- Identification and Authentication (I&A): This security mechanism is used to ensure that only authorized users have access to the COE system resources and that system users can be held individually accountable for their actions. Users are identified to a COE system component using a user ID that must be authenticated by presenting a valid password before permission is granted for accessing system resources or data. The I&A activities that apply to the general user are logging in and out and changing passwords.
- Discretionary Access Control (DAC): This feature allows the user to determine who (owner, group, or world) is able to read, write, or execute a system object (files, directories, pipes, etc.). Authorized users will have access only to system objects granted by DAC controls. Users are also able to specify the access allowed to file system objects that they own. Users must be aware of the proper use of commands that specify DAC access..
- Audit event generation: The fact that audit events are generated when specified commands are executed is transparent to users.

4.2 Identification and Authentication

The security staff provides each new regular user with a unique user ID and password. When the user logs onto the COE system for the first time, the user is required to change the password immediately so that only the user knows the password. The COE password policy enforces selection of appropriate passwords. This password construction validation is provided by software transparent to the user and may be modified by each site to meet its own system requirements. If you attempt to select a password that does not satisfy the password policy of the system, your password will be rejected and you will be asked to select a different password.

Users logging into the COE systems should take the time to read and understand the information displayed on the login banner. The banner describes the security nature of the environment, proper behavior while operating in this environment, and the security guidelines defining its operation. The following banner is representative of what is presented:

THIS IS A DEPARTMENT OF DEFENSE (DOD) INTEREST COMPUTER SYSTEM. ALL DOD INTEREST COMPUTER SYSTEMS AND RELATED EQUIPMENT ARE INTENDED FOR THE COMMUNICATION, TRANSMISSION, PROCESSING, AND STORAGE OF OFFICIAL U.S. GOVERNMENT OR OTHER AUTHORIZED INFORMATION ONLY. ALL DOD INTEREST COMPUTER SYSTEMS ARE SUBJECT TO MONITORING AT ALL TIMES TO ENSURE PROPER FUNCTIONING OF EQUIPMENT AND SYSTEMS INCLUDING SECURITY DEVICES AND SYSTEMS, TO PREVENT UNAUTHORIZED USE AND VIOLATIONS OF STATUTES AND SECURITY REGULATIONS, TO PREVENT CRIMINAL ACTIVITY, AND FOR OTHER SIMILAR PURPOSES. ANY USER OF A DOD INTEREST COMPUTER SYSTEM SHOULD BE AWARE THAT ANY INFORMATION PLACED IN THE SYSTEM IS SUBJECT TO MONITORING AND IS NOT SUBJECT TO ANY EXPECTATION OF PRIVACY. IF MONITORING OF THIS OR ANY OTHER DOD INTEREST COMPUTER SYSTEM REVEALS POSSIBLE EVIDENCE OF VIOLATION OF CRIMINAL STATUTES, THIS EVIDENCE AND ANY OTHER RELATED INFORMATION, INCLUDING IDENTIFICATION INFORMATION ABOUT THE USER, MAY BE PROVIDED TO LAW ENFORCEMENT OFFICIALS. IF MONITORING OF THIS OR ANY OTHER DOD INTEREST COMPUTER SYSTEM REVEALS VIOLATIONS OF SECURITY REGULATIONS OR UNAUTHORIZED USE, EMPLOYEES WHO VIOLATE SECURITY REGULATIONS OR MAKE UNAUTHORIZED USE OF DOD INTEREST COMPUTER SYSTEMS ARE SUBJECT TO APPROPRIATE DISCIPLINARY ACTION.
USE OF THIS OR ANY OTHER DOD INTEREST COMPUTER SYSTEM CONSTITUTES A CONSENT TO MONITORING AT ALL TIMES"

Figure 4.2.-1 DoD Login Warning Banner

4.2.1 Password Construction

Passwords are the primary method for user I&A. Bad passwords are one of the principal means that a hacker will use to break into systems. Therefore, properly constructed passwords are an essential aspect of maintaining system security.

The following general rules apply to constructing a password:

- Users are responsible for protecting their secret passwords against loss or disclosure and will be held liable for any improper use of the password.
- User-generated passwords are required to have the following characteristics:
  - Be at least eight characters in length.
  - Contain at least six alphabetic characters and two numbers or special characters.
  - May not be a password that was used within the previous three password changes.
  - May not include a word found in a dictionary or a name, spelled forwards or backwards.

- May not be a simple keyboard sequence, such as asdfghjkl, or repetitions of the user ID (e.g., user ID is ann; password is annann12).

In addition to the required minimum characteristics, the user may also choose to include upper and lower case letters in the password.

The best way to create passwords is through word links. To choose a good password, try one of the following techniques:

- Combine several short words with numbers or special characters; for example, jumP;0ut. (Notice that the last half of the sample password is composed with a zero in "out".)
- Use an acronym derived from an easily remembered phrase. For example, the phrase "The house on the corner is well maintained" translates to the acronym Thotciwm. Try to use phrases that are not well known or famous quotes.
- Use a nonsense word that is pronounceable.

4.2.2 Password Lifetime

Password lifetime (also known as password aging) refers to how long a password is valid on the system. For COE systems, the maximum lifetime of a password on the system is 91 days. Therefore, users must change their passwords at least every 91 days. You will be prompted to change your password as the current password nears expiration. If you do not change your password before it expires, you will need to see your security administrator to unlock your account and create a new (temporary) password. You will then need to immediately select a new password that is only known to you.

The minimum password lifetime is 7 days. Users must wait at least 7 days to change their password from a previous password change. If a password change is required sooner because of a suspected compromise of the account, contact the site Security Manager to reset the password.

4.2.3 Password Monitoring

Passwords on the system are monitored to check the strength of each password. Users should ensure they have a properly constructed password that does not leave the system vulnerable to hacking.

4.2.4 Account Lockout

If a user cannot login to the system, he or she should contact the security staff for further guidance. The security staff may have detected a bad password and disabled the user account. Users should also be aware that if they enter an incorrect username and/or password three times, their account may be locked. To unlock an account, users must see their security administrator.

4.3 Discretionary Access Control

File owners are responsible for controlling and protecting access to the files that they create and own. As the owner/creator, a user must consider other user's need-to-know prior to allowing access to file system object. Improperly controlled file access can permit unauthorized users improper access to information and potentially compromise system security.

The user must ensure that permissions on his/her home directory conform to the least privilege concept. The user home directory is the user's workspace. It must be maintained in accordance with system security policy and requirements. It is important for the user to understand that the permissions on objects created within the home directory should restrict access exclusively to the user. Sharing objects within the user's home directory requires that permissions on the directory allow another user access to the objects.

NOTE: Before setting permissions on any files under a user's control, the user should discuss the implications of the change with the security staff.

4.4 User Audit Monitoring

The security staff performs auditing on a regular basis. Users must be aware that they are responsible for their actions on the system. They should notify the security staff of any security-related issues, such as if their password may have been compromised.

5. USER SECURITY ACTIVITIES

5.1 UNIX Platforms

The Common Desktop Environment (CDE) executes on the UNIX systems and provides a single common desktop interface for the COE system users. The CDE provides simplified access to applications in a streamlined and intuitive way, and point-and-click flexibility within a single graphical user interface.

5.1.1 Logging In to a COE System

To login to the system:
1. At the Name prompt, enter user ID.
2. At the Password prompt, enter the user's password.

Once successfully logged on, the desktop appears (Figure 5.1.1.-1).

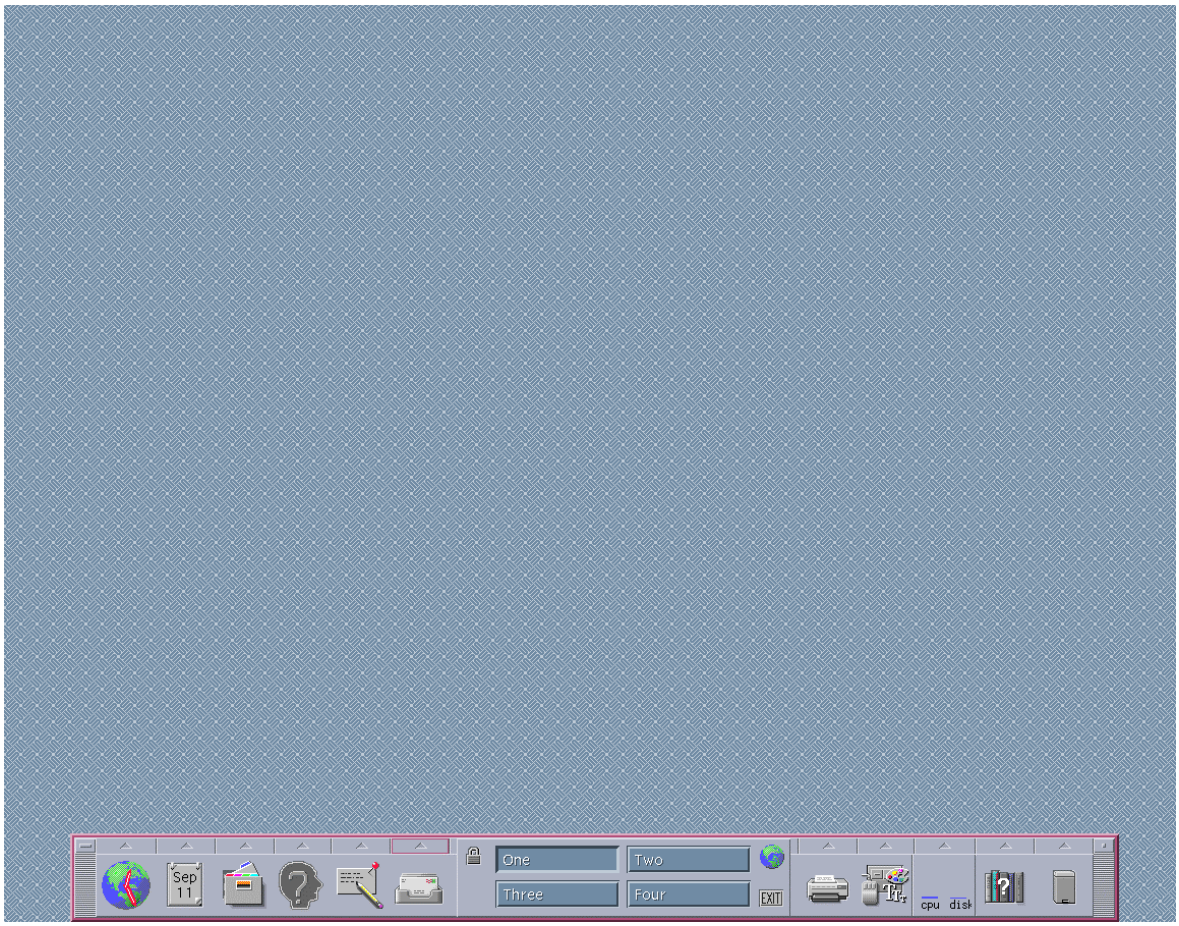

Figure 5.1.1.-1. UNIX Common Desktop Environment

5.1.2 Logging Off a COE System

To logoff the system, either:
1. Select the **Exit** button at the bottom of the screen
2. Choose **Continue to Logout** in the confirmation window that is subsequently displayed

OR,

1. Click the right mouse button
2. Select **Logout**
3. Choose **Continue to Logout** in the confirmation window that is subsequently displayed.

5.1.3 Changing Passwords

To change passwords:
1. Click the arrow button above the Profile Selector icon (the icon with the silhouette and a question mark overlaid on it (See Figure 5.1.3.-1).

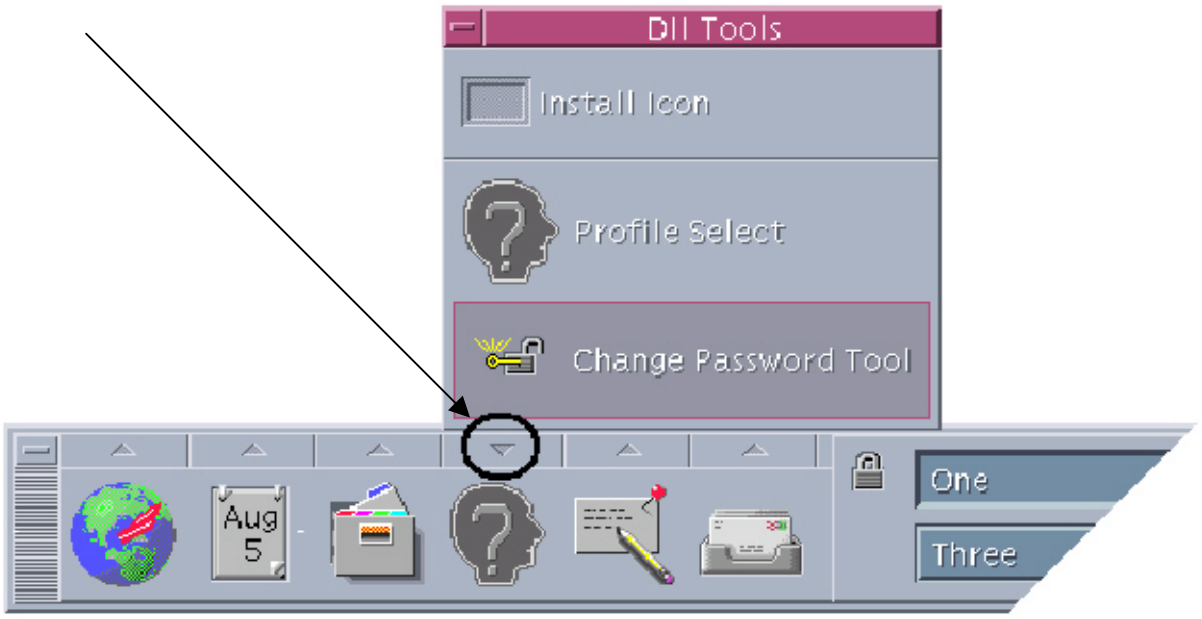

Figure 5.1.3.-1 Selecting the Change Password Tool

2. Click on the Change Password Tool
3. When the "Change you password" dialog box appears, enter the old and new passwords (See Figure 5.1.3.-2).
4. Enter the new password in the Password Confirm field.

Figure 5.1.3.-2 Change Your Password Dialog Box

NOTE: It is strongly recommended that a user change his/her password on ALL machines within the COE administrative domain at one time. Password synchronization problems may occur if passwords are changed on individual machines within a COE domain. See Section 5.3 for additional details.

5. Select the host(s) on which to change your password. Figure 5.1.3.-3 depicts a password change on an individual host.

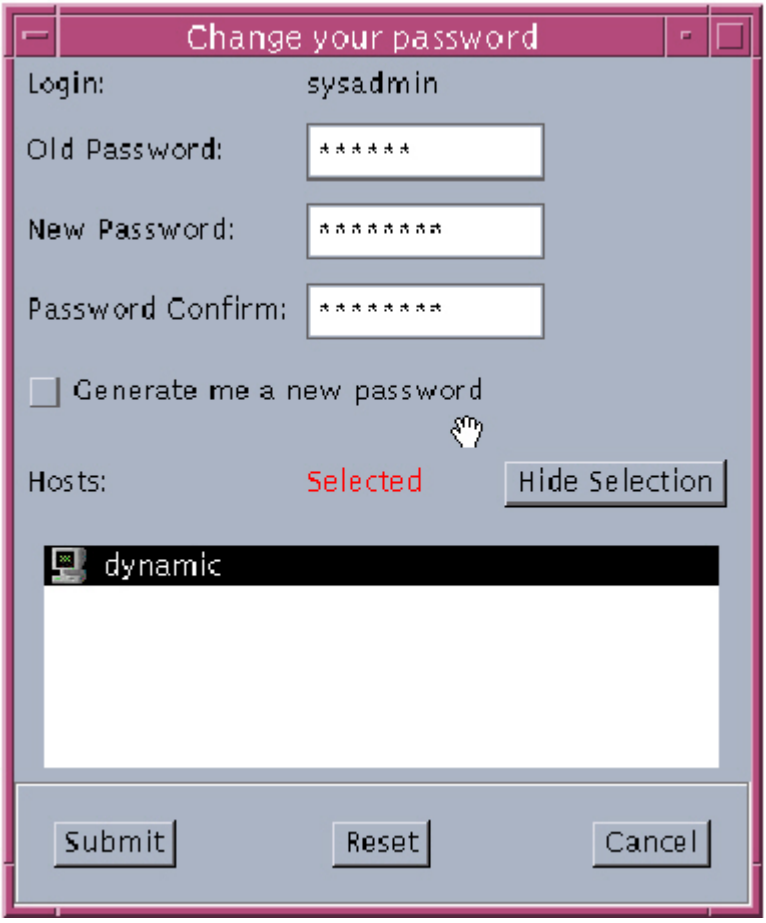

Figure 5.1.3.-3 Password Change On an Individual Host

6. Select the **Submit** button at the bottom of the dialog box.
7. A Status Summary dialog box will confirm the password change (See Figure 5.1.3.-4).

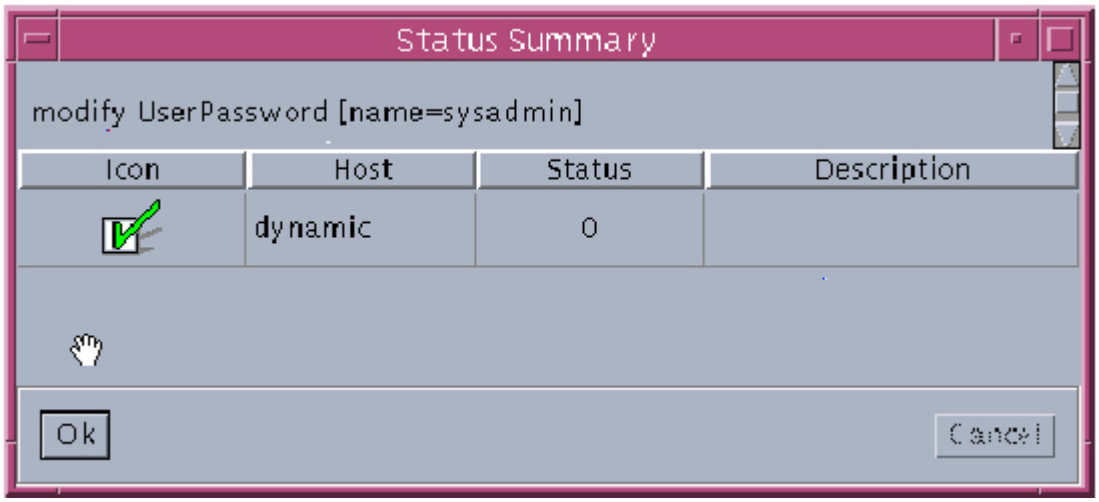

Figure 5.1.3.-4 Status Summary of Password Change

5.1.4 Profile Selection

Profiles define the menu and icon access, and user environment for each COE system user. Users may be given more than one profile depending on their duties and responsibilities.

To select a profile:

1. Click on the **Profile Selector** icon at the bottom of the screen. The Profile Selector icon is the icon with the silhouette and a question mark overlaid on it (Figure 5.1.4.1)

Figure 5.1.4-1 Common Desktop Environment – Profile Selector Icon

2. Click on the desired profile from the "Available Profiles" list.

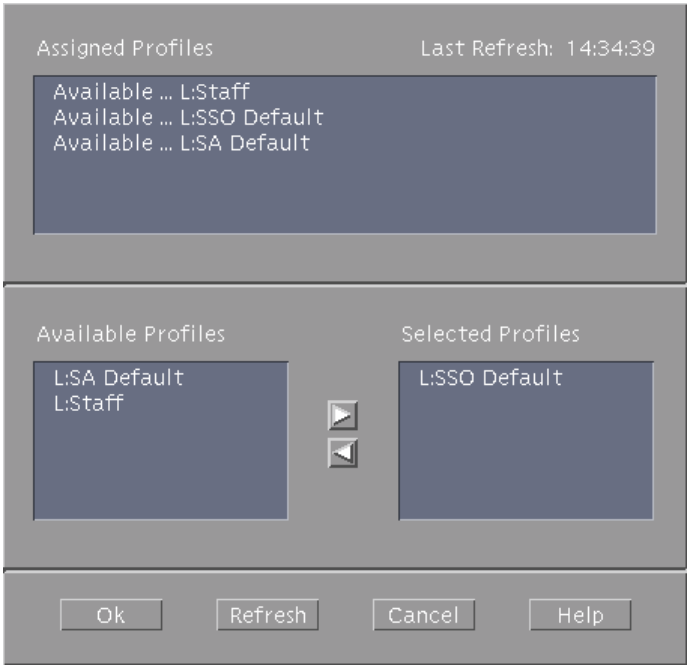

Figure 2.1.4-2 Profile Selector

3. Press the right-pointing arrow to move the selected profile from the "Available Profiles" to the "Selected Profiles" list.
4. Click on **OK**.
5. Another window will open verifying your selection. Click **OK**.

5.1.5 File and Directory Permissions

File and directory management is a feature provided through the CDE. To change permissions on user controlled files or directories:

1. Click on the **File Manager** icon at the bottom of the screen.

Figure 5.1.5-1. Common Desktop Environment – File Manager Icon

2. A window similar to that shown in Figure 5.1.5-2 will appear. Click on the file whose permissions you want to alter.

Figure 5.1.5.-2. File Manager

3. Click on **Selected** at the top of the window.
4. Click on **Change Permission**.
5. Change the permissions to the desired permissions (See Figure 5.1.5.-3).

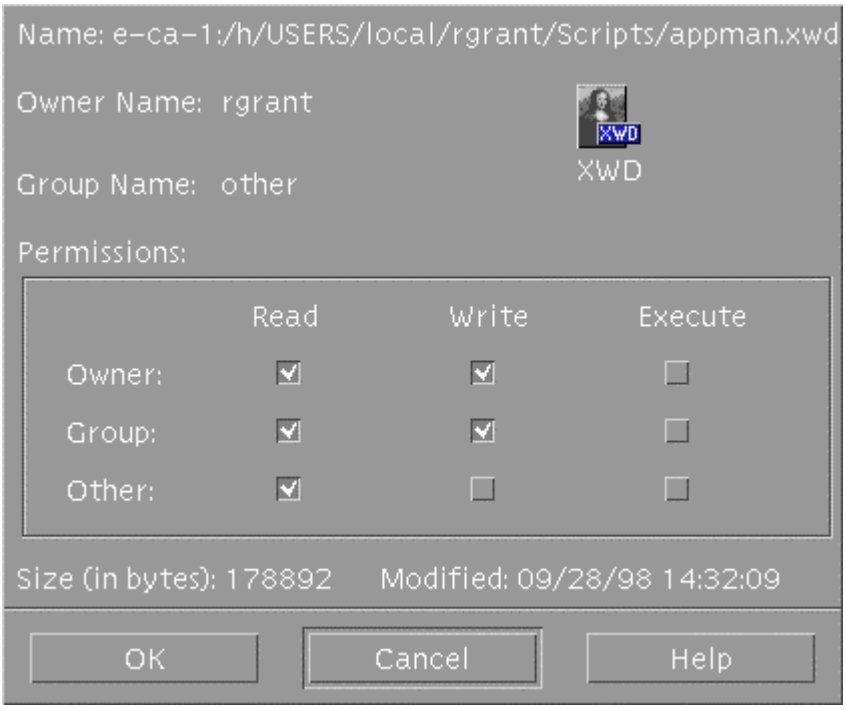

Figure 5.1.5-3. Assigning File Permissions

6. Click on **OK** to continue.

5.2 NT Platform

5.2.1 Logging In to a COE System

All users must first login to a Windows NT system before being allowed access to any system resources. To login, users must first hit the CTRL+ALT+DEL keys simultaneously. The DoD Login Warning Banner will appear. Select OK to receive the login dialog box. The user then enters his or her username and password. The selection made in the "Domain" pull-down list defines which account the user is attempting to login to (e.g., an account on the local machine or an account in a domain to which the computer belongs).

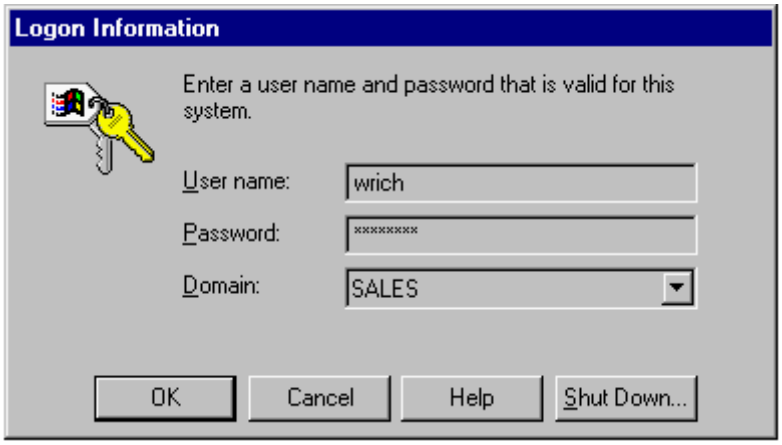

Figure 5.2.1.-1 Windows NT Logon Information Dialog Box

5.2.2 Logging Off a COE System

When leaving a workstation for any length of time, users should either log off or lock the workstation in order to protect the workstation and the user's data from passers by who can take advantage of the open session.

Logging off a workstation allows other users with valid accounts to use the machine without disrupting the previous user data, whereas locking the workstation locks the interactive user interface but does not close the currently logged in user's processes.

To logoff a COE system, press CTRL+ALT+DEL and then choose the "Logoff" button in the Windows NT Security dialog box. A pop-up dialog box will confirm if you wish to end your NT session; choose OK to continue the logoff.

To manually lock your workstation, press CTRL+ALT+DEL and then choose the "Lock Workstation" button in the Windows NT Security dialog box. To unlock your workstation press CTRL+ALT+DEL and type your password into the "Workstation Locked" dialog box.

5.2.3 Changing Passwords

1. Click on the Start menu button at the bottom of the screen.
2. Click on the Change Password Tool.

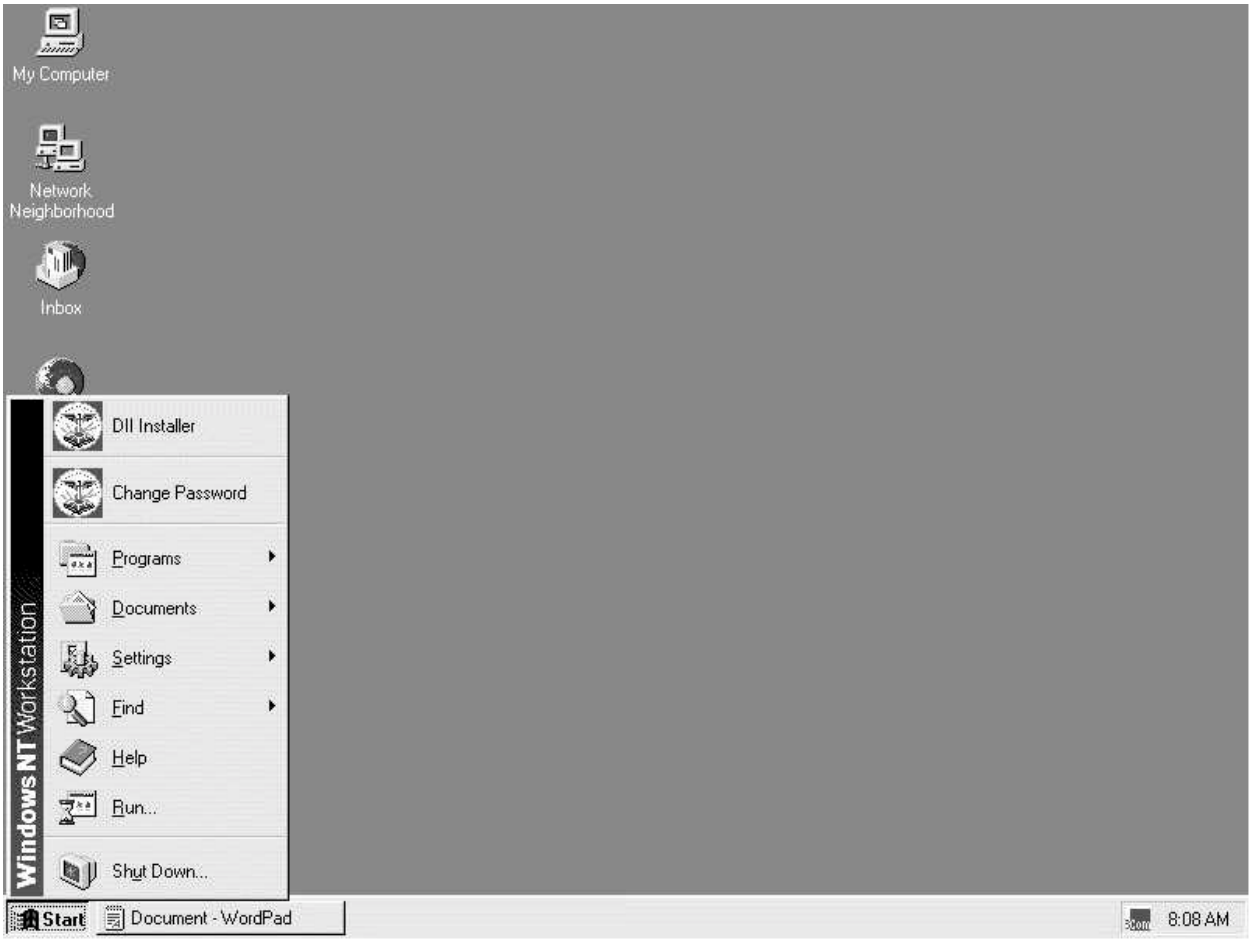

Figure 5.2.3.-1 Windows NT COE Change Password Tool

3. When the "Change you password" dialog box appears, enter the old and new passwords (See Figure 5.1.3.-2).
4. Enter the new password in the Password Confirm field.

Figure 5.2.3.-2 Windows NT COE Change Your Password Dialog Box

NOTE: It is strongly recommended that a user change his/her password on ALL machines within the COE administrative domain at one time. Password synchronization problems may occur if passwords are changed on individual machines within a COE domain. See Section 5.3 for additional details.

5. Select the host(s) on which to change your password.
6. Select the **Submit** button at the bottom of the dialog box.
7. A Status Summary dialog box will confirm the password change (See Figure 5.1.3.-4).

5.2.4 Profile Selection

When a user has been authenticated and established a session, he or she sees a familiar desktop with applications and settings that are the same as the last time he or she logged on. This collection of assigned applications and settings is called a profile. Windows NT 4.0 assigns these User Profiles to each valid user. NT can create two principal types of User Profiles (Local and Roaming) as described below.

5.2.4.1 Local

Local profiles are specific to the local machine on which they are created. One machine can store multiple profiles for multiple users who log onto that workstation. A local profile is user and computer specific. It is created when a user first logs on at a Windows NT computer, and is used when a user does not have a roaming profile.

5.2.4.2 Roaming

Roaming profiles are stored on a network server and accessed when a user logs on. These allow users to maintain a personal desktop on any machine on the network. One advantage of server-

based profiles is that the profile environment will follow the user, no matter what Windows NT computer is used for logon. Roaming profiles are categorized into two types: personal and mandatory. A user can have either a personal profile or a mandatory profile, but not both at the same time.

A personal profile allows a user to change his or her profile. Every time a user logs off, the profile is updated with the current settings. When the same user logs on again, the profile is loaded as last saved. If a personal profile is not available when a user logs on, their local profile will be used.

Mandatory profiles are stored on a network server and preconfigured by the local administrator. These profiles allow administrators to control the desktop of all users participating in the domain. Users with mandatory profiles are given standardized desktops, which they **cannot** change. Any environment changes made by users during a session are not saved to their mandatory profile. If an assigned mandatory profile is not available when a user tries to log on, the user will not be allowed to log on.

5.2.5 File and Directory Permissions

The Windows NT operating system provides the ability to specify access control permissions on files and directories, which are referred to as objects. Each object has an ACL (Access Control List) that identifies the user or group accounts that have been granted access and type of access to the object. When a user requests an action on an object, he or she must have an entry in the object's ACL. Each object has a pair of ACLs, a Discretionary ACL (DACL), and a System ACL (SACL). The DACL specifies permissions that have been assigned to users. The SACL specifies which user operations will be logged in the security audit log. The SACL is set by the system security staff. It is important for users to specify appropriate access control rules for the files they own to prevent unauthorized access to their files.

The following table lists the available permissions a user can set on files and directories along with the effect of each permission. Users can set the permissions on any objects that they own or to which they have been granted Full Control.

Table 5.2.5-1. Object Permission Definitions

Permission	Effect
No Access	Prevents any access to the directory and its file event if the user has been granted full level control.
List	Allows the viewing and browsing of a directory, without access to files unless overridden by other file or directory permissions.
Read	Allows opening files and executing applications.
Add	Allows the adding of files and subdirectories without read access.
Change	The combination of Add and Read permissions, plus Delete.
Full Control	The combination of Add, Read, Delete, and Change, plus taking ownership and assigning permissions.

In order to assign permissions to files and/or directories, users must own or have full control over that object. To edit file or directory permissions, perform the following steps:

1. Open "My Computer"
2. Select and right-click on the target directory or file

Select "Properties", then "Security", then "Permissions".

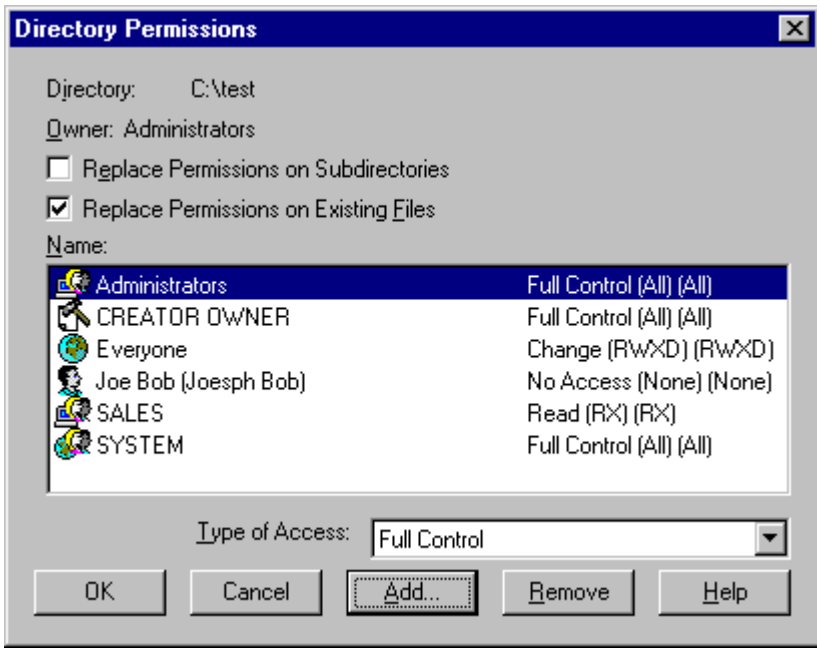

Figure 3.2.5-1 Setting Directory Permissions

The applicable permissions window (
Figure 3.2.5-1 and Figure 5.2.5-2) displays the users and groups with their permissions.

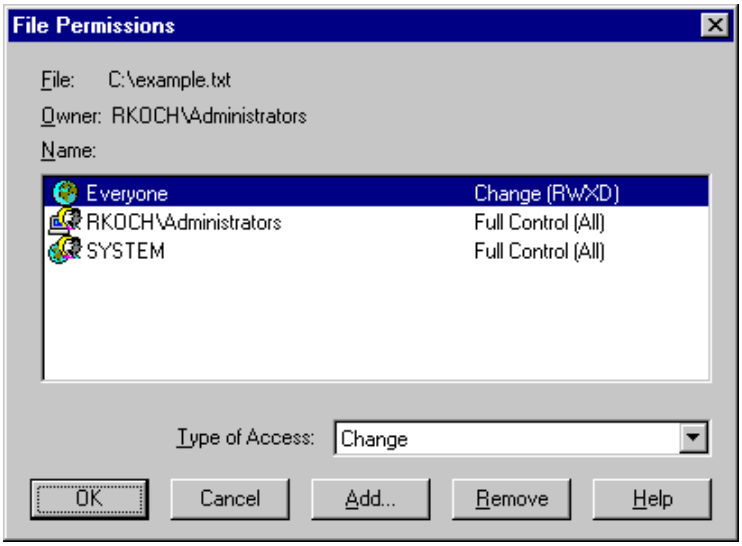

Figure 5.2.5-3 Setting File Permissions

Permissions can be changed by selecting the user/group and clicking and selecting the new access from the "Type of Access:" list.

To grant access to another user, click on the "Add" button. From here, you can add users or groups from the local machine, or if connected to a domain, users or groups from the domain or other trusted domains. To remove another user's access, select the appropriate entry from the list and click on the "Remove" button.

NOTE: When setting permissions on directories, selecting "Replace Permissions on Subdirectories" and "Replace Permissions on Existing Files" will cause the new permissions to be propagated down the entire directory tree. This option should be exercised with caution.

File sharing allows users to access resources available on other machines on a network. Depending on the network configuration, network shares can be seen within local domains as well as remote trusted domains. COE systems are configured such that shares can only be created by the security staff. If a user has a requirement to set up a share, the user should see his/her system administrator.

5.3 COE Administrative Domain

Users must exercise caution when changing their password within a COE Administrative Domain to ensure password consistency. Users are encouraged to follow the steps outlined in Figure 5.3.-1.

Note: If the minimum password age has not elapsed on all computers within the COE domain, some computers will have the new password and some will continue to have the old password. The account password cannot be synchronized across the domain until the minimum password age (7 days) has elapsed on every computer.

If a user is unable to change his/her password on all machines within the domain, there are two options:

1. The user can wait until the minimum password age expires on all computers and then change the password on all hosts; or
2. The site Security Manager (secman account) can run Assign Passwords to expire the user's password, and then the user can start the password change process over.

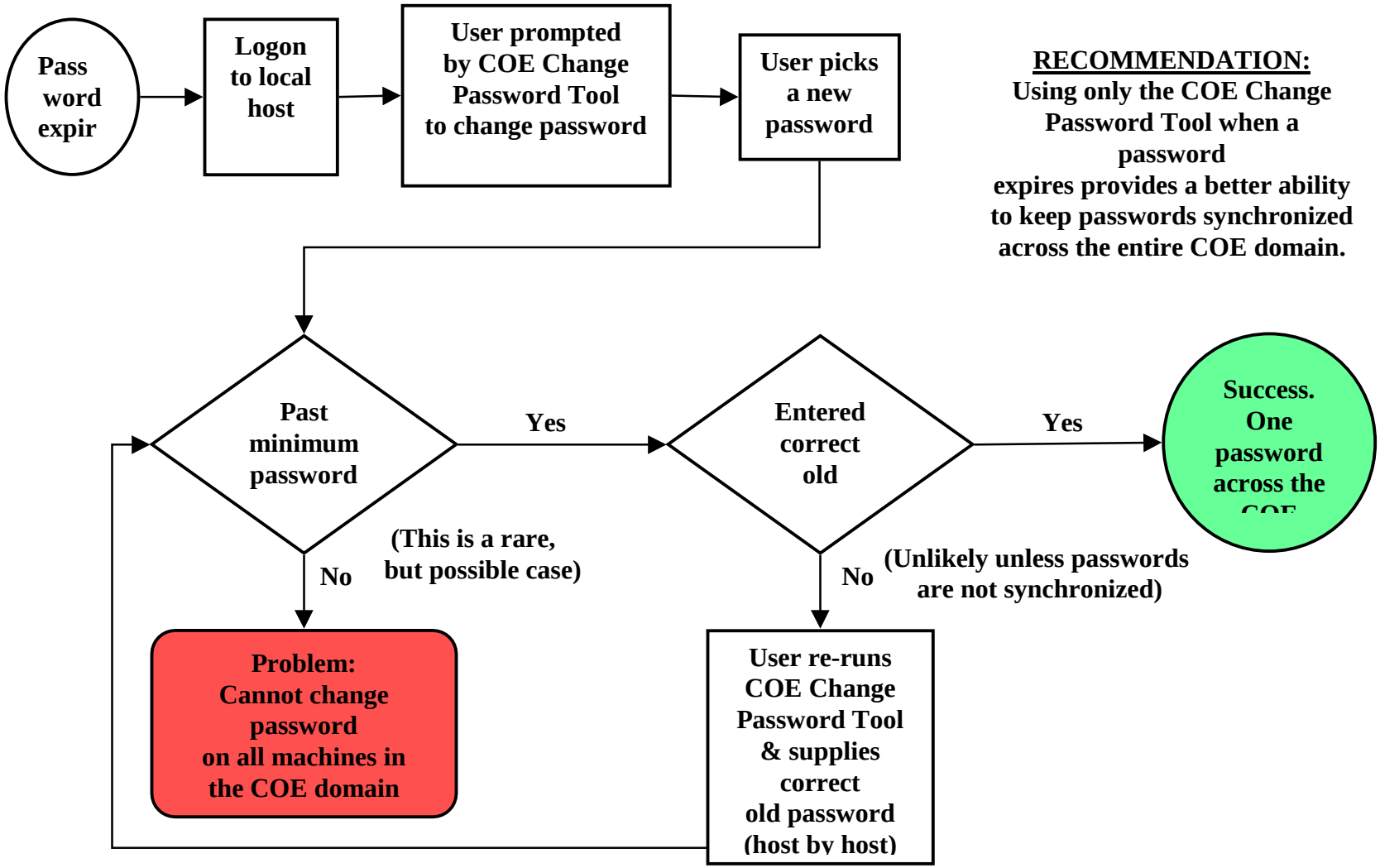
Pass word expir
Logon to local host
User prompted by COE Change Password Tool to change password
User picks a new password
RECOMMENDATION:
Using only the COE Change Password Tool when a password expires provides a better ability to keep passwords synchronized across the entire COE domain.
Past minimum password
Yes
Entered correct old
Yes
Success. One password across the
(This is a rare, but possible case)
No
No
(Unlikely unless passwords are not synchronized)
Problem: Cannot change password on all machines in the COE domain
User re-runs COE Change Password Tool & supplies correct old password (host by host)

Figure 5.3.-1 Password Change Within a COE Administrative Domain

APPENDIX A
ACRONYMS/ABBREVIATIONS

A. ACRONYMS/ABBREVIATIONS

CDE	Common Desktop Environment
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CM	Configuration Management
COE	Common Operating Environment
COTS	Commercial off-the-shelf
DAC	Discretionary Access Control
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
FTP	File Transfer Protocol
GOTS	Government off-the-shelf
GUI	Graphical User Interface
I&A	Identification and Authentication
JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability and Engineering Organization
JS	Joint Staff
LAN	Local Area Network
MS	Microsoft
NFS	Network File System
NIS	Network Information System
NIS+	Network Information Service Plus
OS	Operating System
PC	Personal Computer
RDBMS	Relational Database Management System
RPC	Remote Procedure Call
rsh	Remote Shell
rlogin	Remote Login
SA	Site Administrator
SAG	Site Administrators Guide
SAM	System Administration Manual
SFUG	Security Features User's Guide
SIPRNET	Secret Internet Protocol Router Network
SSIP	Site Security Implementation Procedures
SSOP	Site Standard Operating Procedures
XDM	X Display Manager